PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : E05B 49/00 — A1

(11) Internationale Veröffentlichungsnummer: WO 00/12846

(43) Internationales Veröffentlichungsdatum: 9. März 2000 (09.03.00)

(21) Internationales Aktenzeichen: PCT/DE99/02619

(22) Internationales Anmeldedatum: 20. August 1999 (20.08.99)

(30) Prioritätsdaten:

PP 5515	27. August 1998 (27.08.98)	AU
PP 7489	3. Dezember 1998 (03.12.98)	AU
42419/99	2. August 1999 (02.08.99)	AU

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: ROBERT BOSCH GMBH [DE/DE]; Postfach 30 02 20, D–70442 Stuttgart (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHMITZ, Stephan [DE/DE]; Werderstrasse 24, D–50672 Köln (DE). CROWHURST, Peter [NZ/AU]; 9 Fernlea Avenue, Rowville, VIC 3178 (AU).

(81) Bestimmungsstaaten: BR, JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

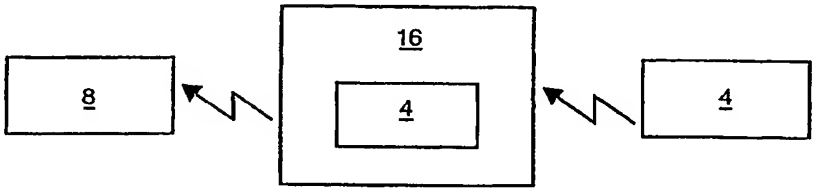
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: SECURITY SYSTEM

(54) Bezeichnung: EIN SICHERHEITSSYSTEM

(57) Abstract

The invention relates to a security system, comprising an electronic key with a transmitter and a secured object with a receiver. The transmitter and the receiver are configured in such a way that they can communicate with each other in order to transfer authentication data. The inventive system is characterised in that the transmitter sends identification data which are unequivocal for the key, said identification data being embedded in the hardware of the transmitter. If the transmitted identification data correspond to the identification data of the receiver, the security system gives authorisation for the secured object when the authentication data are transmitted. The invention also relates to a security system comprising an electronic key with a transmitter and a secured object with a receiver, the transmitter and the receiver being configured in such a way that they can communicate with each other so that authentication data can be transmitted. The authentication data are contained in a reply message which is transmitted by the key in response to an identification request received by the secured object. The system is characterised in that at least a part of the reply message must be received within a time slot for acceptance for the authorisation for the secured object to be given by the security system, said time slot beginning a set period of time after the start of the transmission of the identification request.



BEST AVAILABLE COP

(57) **Zusammenfassung**

Ein Sicherheitssystem, welches einen elektronischen Schlüssel mit einem Sender und einen gesicherten Gegenstand mit einem Empfänger einschliesst, worin der Sender und der Empfänger so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten zu übertragen, dadurch gekennzeichnet, dass der Sender Identifizierungsdaten übermittelt, die für den Schlüssel eindeutig sind, wobei die Identifizierungsdaten in Hardware des Senders eingebettet sind und das Sicherheitssystem eine Befugnis für den gesicherten Gegenstand bei Übertragung der Authentifizierungsdaten gewährt, wenn die übertragenen Identifizierungsdaten den Identifizierungsdaten des Empfängers entsprechen. Ein Sicherheitssystem, welches einen elektronischen Schlüssel mit einem Sender und einen gesicherten Gegenstand mit einem Empfänger einschließt, wobei der Sender und des Empfänger so ausgelegt sind, dass sie miteinander kommunizieren, um Authentifizierungsdaten zu übertragen, worin die Authentifizierungsdaten in einer Antwortnachricht enthalten sind, die von dem Schlüssel in Beantwortung einer von dem gesicherten Gegenstand empfangenen Kennungsabfrage übertragen wird, dadurch gekennzeichnet, dass mindestens ein Teil der Antwortnachricht innerhalb eines Abnahmezeitausschnitts empfangen werden muss, damit die Befugnis von dem Sicherheitssystem für den gesicherten gegenstand erteilt wird, wobei der Abnahmezeitausschnitt zu einer vorbestimmten Zeitperiode ab dem Übertragungsbeginn der Kennungsabfrage beginnt.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

BEST AVAILABLE COPY

EIN SICHERHEITSSYSTEM

Die vorliegende Erfindung bezieht sich auf ein Sicherheitssystem, insbesondere ein passives Sicherheitssystem für Fahrzeuge.

Derzeit existierende passive Sicherheitssysteme für den Zugang und die Aktivierung von Fahrzeugen verwenden fernbetätigte elektronische Schlüssel, die einen Sender einschließen, der Authentifizierungsdaten an einen in dem Fahrzeug befindlichen Empfänger übermittelt, wenn der Schlüssel innerhalb eines vorbestimmten Bereichs des Empfängers ist. Das zwischen dem Sender und dem Empfänger aktivierte Kommunikationsprotokoll benutzt zum Führen der übertragenen Daten eine Radiofrequenz-Schnittstelle. Die Radiofrequenz (RF)-Schnittstelle hat einen begrenzten Bereich, um zu gewährleisten, daß die Kommunikationsverbindung unterbrochen wird, wenn sich eine im Besitz des Schlüssels befindliche Person aus der unmittelbaren Nähe des Fahrzeugs entfernt.

Passive Sicherheitssysteme sind leicht Angriffen unbefugter Personen ausgesetzt, die Abfangeinrichtungen benutzen, die in die Nähe des Fahrzeugs und des Schlüssels gebracht werden, um die von dem Schlüssel übermittelten Übertragungen zu empfangen und die Übertragungen an das Fahrzeug weiterzuübertragen oder die Übertragungen aufzuzeichnen. Wenn die Übertragungen erst einmal abgefangen worden sind, können sie demoduliert werden, um die übertragenen Daten zu erhalten. Eine unbefugte Person kann einen authentischen Schlüssel von dem Hersteller erwerben und die übertragenen Daten mit dem erworbenen Schlüssel als einem Zweitschlüssel benutzen. Dieser Zweitschlüssel kann dann verwendet werden, um unbefugten Zugang zu erlangen und/oder das Fahrzeug zu benutzen. Es soll mit der vorliegenden Erfindung ein

System vorgestellt werden, welches dieses Problem beseitigt oder welches zumindest eine zweckmäßige Alternative bietet.

Die vorliegende Erfindung stellt ein Sicherheitssystem vor, welches einen elektronischen Schlüssel mit einem Sender und einen gesicherten Gegenstand mit einem Empfänger einschließt, wobei der Sender und der Empfänger so ausgelegt sind, daß sie miteinander kommunizieren, um Authentifizierungsdaten zu übertragen, dadurch gekennzeichnet, daß der Sender Identifizierungsdaten übermittelt, die für den Schlüssel eindeutig sind, wobei die Identifizierungsdaten in Hardware des Senders eingebettet sind, und das Sicherheitssystem eine Befugnis für den gesicherten Gegenstand bei Übertragung der Authentifizierungsdaten gewährt, wenn die übertragenen Identifizierungsdaten den Identifizierungsdaten des Empfängers entsprechen.

Die vorliegende Erfindung stellt auch ein Sicherheitssystem vor, einschließlich einen elektronischen Schlüssel mit einem Sender und einen gesicherten Gegenstand mit einem Empfänger, wobei der Sender und der Empfänger so ausgelegt sind, daß sie miteinander kommunizieren, um Authentifizierungsdaten zu übertragen, wobei die Authentifizierungsdaten in einer Antwortnachricht eingeschlossen sind, die von dem Schlüssel in Antwort auf eine von dem gesicherten Gegenstand erhaltenen Kennungsabfrage übertragen wird, dadurch gekennzeichnet, daß mindestens ein Teil der Antwortnachricht innerhalb eines Abnahmezeitausschnitts erhalten werden muß, damit das Sicherheitssystem eine Befugnis für den gesicherten Gegenstand gewährt, wobei der Abnahmezeitausschnitt zu einer vorbestimmten Zeitperiode ab dem Übertragungsbeginn der Kennungsabfrage beginnt.

Die vorliegende Erfindung stellt ein Sicherheitssystem vor, welches einen elektronischen Schlüssel mit einem Sender und einen gesicherten Gegenstand, in welchem sich ein Empfänger befindet, einschließt, wobei der Sender und der Empfänger so ausgelegt sind, daß sie miteinander kommunizieren, um Authentifizierungsdaten zu übertragen, dadurch gekennzeichnet, daß das von dem Sender und dem Empfänger ausgeführte Kommunikationsprotokoll die Übertragung der Authentifizierungsdaten durch einen unbefugten Sender erkennt.

Eine bevorzugte Realisierung der vorliegenden Erfindung ist anschließend mit Bezug auf die beiliegenden Zeichnungen als Beispiel beschrieben, wobei:

Figur 1 eine schematische Ansicht einer bevorzugten Realisierung eines Sicherheitssystems mit einer Abfangstation ist;

Figur 2 ein Blockdiagramm des Sicherheitssystems ist; und

Figur 3 ein Zeitdiagramm für von dem Sicherheitssystem übermittelte Signale ist.

Ein passives Sicherheitssystem 2, wie in den Figuren gezeigt, schließt folgende ein:
einen elektronischen Schlüssel 4 mit einem Sender 6 und einer Induktionsspulenantenne 7, eine Basisstation 8 mit einem Empfänger 10 und einer Induktionsspulenantenne 12. Die Basisstation 8 ist an einem gesicherten Ort untergebracht, wie z.B. einem Fahrzeug, und kontrolliert den Zugang zu dem gesicherten Ort und/oder das Starten des Fahrzeugs. Wenn der Schlüssel 4 innerhalb eines bestimmten Bereichs der Antenne 12 des Empfängers 10 herangeführt wird, erregt der Empfänger 10 den Schlüssel 4, und veranlaßt dadurch den Sender 6, die Übermittlung an den Empfänger 10 zu beginnen. Daten

werden unter Verwendung von RF-Signalen übermittelt, welche eine Kommunikationsverbindung zwischen dem Schlüssel 4 und der Basisstation 8 herstellen. Die zwischen dem Schlüssel 4 und der Basisstation 8 übermittelten Daten werden durch ein Kommunikationsprotokoll bestimmt, welches der Schlüssel 4 und die Basisstation 8 befolgen, und welches die Übermittlung von Authentifizierungsdaten von dem Schlüssel 4 an den Empfänger 10 beinhaltet. Zugang zu dem gesicherten Ort und/oder Starten des Fahrzeugs wird von der Basisstation 8 nur dann zugelassen, wenn die übermittelten Authentifizierungsdaten mit den von der Basisstation 8 gespeicherten Authentifizierungsdaten übereinstimmen.

Eine Abfangstation 16 schließt einen Empfänger ein, um auch die Übertragungen von dem Schlüssel 4 zu empfangen und alle empfangenen Signale zu speichern oder weiterzuübertragen. Die Station 16 wird benutzt, um die übertragenen Signale zu demodulieren, um eine Kopie der übertragtenen Daten zu erhalten. Die Schlüssel 4 sind Massenteile und entsprechen den von Fahrzeugherstellern vorgegebenen Anforderungen.

Die Schlüssel 4 weisen eine Anzahl von Sicherheitsmerkmalen auf, wie zum Beispiel die übertragenen Authentifizierungsdaten und eine eindeutige spektrale Signatur oder einen charakteristischen Auffangpunkt dritter Ordnung (third order intercept point), wie in der Beschreibung der australischen Patentanmeldung Nr. 33933/99 des Antragstellers besprochen. Es ist jedoch möglich, daß ein Unbefugter in der Lage ist, einen der massenproduzierten Schlüssel 4 in seinen Besitz zu bekommen und die mittels der Abfangstation 16 erhaltenen Daten zu benutzen, wobei die Daten einfach an das Fahrzeug weiterübertragen werden können, indem der Sender des erhaltenen unbefugten Schlüssels benutzt wird, oder die Daten können in den unbefugten Schlüssel 4 gespeichert werden, um einen Zweitschlüssel 4 zu erstellen. Der Zweitschlüssel 4 könnte daher dafür

benutzt werden, unbefugten Zugang zu einem Fahrzeug und/oder unbefugte Benutzung eines Fahrzeugs zu erzielen. In einem Weiterübertragungs-Angriff (relay attack) wird die Abfangstation dazu benutzt, den Originalschlüssel 4 zu erregen, welcher sich im Haus/Betrieb des Besitzers befinden kann, und dann die empfangenen demodulierten Daten von dem Originalschlüssel 4 zu dem Fahrzeug weiterzuübertragen unter Verwendung des Senders des Zweitschlüssels 4.

Um derartige Vorkommnisse gemäß der nachfolgend beschriebenen bevorzugten Realisierung zu verhindern, werden die Schlüssel 4 alle mit einer eindeutigen Seriennummer hergestellt, die als Identifizierungsdaten in dem Schlüssel 4 eingeschlossen sind. Die Identifizierungsdaten werden in der Maskenkonfiguration einer integrierten Schaltung untergebracht, welche den Sender 6 des Schlüssels 4 einschließt. Die Identifizierungsdaten sind so in der integrierten Schaltung eingeschlossen, daß sie nach der Anfertigung von keinem anderen elektronischen Bauelement gelesen werden können. Der Sender 6 ist auch so ausgelegt, daß wenn der Schlüssel 4 von der Basisstation 8 erregt wird, die Identifizierungsdaten, welche die Seriennummer darstellen, zuerst übertragen werden, bevor der Sender mit der Übertragung irgendwelcher anderer Daten, die ihm geliefert werden, beginnt, wie z.B. die Authentifizierungsdaten. Zum Beispiel wird der Sender 6 alle Daten übertragen, die er von einem Mikrocontroller 35 empfängt, unter Benutzung eines Kommunikationsprotokolls, welches einen Anfangskennsatz einschließt, der als erster übermittelt wird, bevor irgendwelche anderen Daten übertragen werden. Der Sender 6 schließt in dem Anfangskennsatz die Seriennummer des Schlüssels 4 ein. Die Basisstation 8 führt eine Kopie der eindeutigen Seriennummer und wird nur Zugang zu dem Fahrzeug und/oder Benutzung des Fahrzeugs ermöglichen, falls:

(a) die empfangene Seriennummer mit der in der Basisstation 8 gespeicherten Seriennummer übereinstimmt; und

(b) die Basisstation 8 die übertragene Seriennummer innerhalb einer zulässigen Zeitspanne empfängt.

Die zulässige Zeitspanne entspricht der ersten Anfangsperiode, wenn eine Übertragung von dem Schlüssel 4 empfangen wird. Die zulässige Zeitspanne ist so eingestellt, daß sie den Empfang der übertragenen Seriennummer in der Anfangsübertragung erlaubt, ist aber auch kurz genug eingestellt, daß sie die Unterdrückung der Übertragung der eindeutigen Seriennummer des Zweitschlüssels gefolgt von der Übertragung einer von dem Originalschlüssel kopierten Seriennummer erkennt. Dadurch wird sichergestellt, daß Unbefugte keinen Zugang zu dem Fahrzeug erhalten und/oder das Fahrzeug benutzen können, indem kopierte Daten übertragen werden, welche die Seriennummer des kopierten Originalschlüssels einschließen, nachdem die Übertragung der Seriennummer von dem Zweitschlüssel unterdrückt wurde. Durch Verwendung des Kommunikationsprotokolls mit dem die Seriennummer übermittelnden Anfangskennsatz, wird bei einem Weiterübertragungs-Angriff die Abfangstation 16, welche den unbefugten Schlüssel 4 benutzt, zuerst den Anfangskennsatz einschließlich der Seriennummer des unbefugten Schlüssels senden, gefolgt von dem Anfangskennsatz und den von dem Originalschlüssel 4 erhaltenen Daten. Die Übertragung von zwei Anfangskennsätzen, oder in der Tat zwei Seriennummern, wird erkannt. Die zulässige Zeitspanne stimmt daher mit der Zeit überein, die in Anspruch genommen wird, um einen Anfangskennsatz zu übertragen, bevor irgendwelche Daten empfangen werden. Die Struktur des Anfangskennsatzes kann erkannt werden wenn sich eindeutige digitale Speicherworte am Start und Stop eines jeden Anfangskennsatzes befinden. Auch der Anfang der Daten kann erkannt werden, wenn ein eindeutiger Datenvorspann vorhanden ist.

Dementsprechend, durch Erkennung der Anfangskennsätze, wenn die am Empfänger 10 erkannte Anfangskennsatz-Zeitdauer die Länge eines Anfangskennsatzes überschreitet, dann wird der Zugang zu dem Fahrzeug und/oder Benutzung des Fahrzeugs verweigert.

Der Sender 6, wie in Figur 2 gezeigt, beinhaltet eine integrierte Schaltung, die zwei konstante Tonsignale übermittelt, sobald der Schlüssel 4 von dem Empfänger 10 erregt wird. Die Schaltung kann zwei Radiofrequenz-Oszillatoren 30 bzw. 32 für die Töne einschließen, deren Ausgaben in einer Antennenweiche 34 zur Übertragung auf die Antenne 7 des Senders 6 vereinigt werden. Alternativ kann die Schaltung einen komplexen Quadraturmodulator einschließen, der die Erzeugung von zwei Tönen getrennt durch ein Mehrfaches des in dem Empfänger 10 verwendeten Kanalabstands ermöglicht.

Eines der Tonsignale, zum Beispiel das von dem ersten Frequenz-Oszillator 30 erzeugte, wird benutzt, um die Identifizierungsdaten, welche die eindeutige Seriennummer darstellen, zu übermitteln. Der Schlüssel 4 schließt einen Mikrocontroller 35 ein, welcher Daten zur Übertragung an den Sender 6 liefert. Der Sender 6 empfängt die Daten und stellt sie zusammen mit einem Anfangskennsatz einschließlich seiner Seriennummer zur Übertragung an die Basisstation 8 bereit. Der Sender 6 enthält einen Code zum Aufbau eines Anfangskennsatzes and stellt ihn zusammen mit Daten bereit zur Übertragung in Übereinstimmung mit dem Kommunikationsprotokol zwischen dem Schlüssel 4 und der Basisstation 8.

Der Empfänger 10 der Basisstation 8 schließt ein mit der Antenne 12 verbundenes FM Empfangsgerät 36, einen Analog-Digital-Umsetzer 38, einen Mikrocontroller 40 und einen frequenzsynthetisierten lokalen Oszillator 42 ein. Der

Mikrocontroller 40 ist zur Steuerung des Frequenzsynthetisators 42 programmiert, sowie zur Verarbeitung von Daten, die von dem A-D-Umsetzer 38 und dem FM-Empfangsgerät 36 empfangen werden. Der Frequenzsynthetisator wird zum Auswählen der Frequenzkanäle verwendet, die von dem FM-Empfänger 36 verarbeitet werden sollen, der eine RSSI-Ausgabe für jeden der vier Kanäle C1 bis C4 erzeugt, wie in der Spezifikation der australischen Patentanmeldung No. 33933/99 des Antragstellers besprochen. Die RSSI Ausgabe für jeden Kanal wird in den A-D-Umsetzer geleitet zur Umsetzung in ein Binärwort zur Verarbeitung durch den Mikrocontroller 40. Der Mikrocontroller 40 behandelt das Binärwort als spektrale Daten, die für die empfangene Energie in jedem der Kanäle C1 bis C4 repräsentativ ist, und verwendet dann die spektralen Daten zum Vergleich mit einer vorher gespeicherten spektralen Signatur für den Sender 6.

Der FM-Empfänger 36 demoduliert auch die auf einem der Kanäle C2 oder C3 empfangenen Daten, die mit dem Tonsignal übereinstimmen, welches die übertragenen Identifizierungsdaten übermittelt, um irgendeinen Anfangskennsatz mit den Identifizierungsdaten zu erhalten, und es leitet diese an den Mikrocontroller 40 auf einer "Daten-erhalten- Ausgabe" (data received output) weiter. Der Mikrocontroller 40 speichert eine Kopie der eindeutigen Seriennummer des berechtigten Originalschlüssels 4 als Identifizierungsdaten und benutzt diese gespeicherten Daten zum Vergleich mit den übertragenen Identifizierungsdaten.

Das System 2 wird gestartet, indem der Schlüssel 4 innerhalb den vorbestimmten Bereich der Antenne 12 geführt wird, damit der Schlüssel 4 erregt wird und eine Übertragung der zwei Grundtöne und der eindeutigen Seriennummer verursacht. Die von dem Mikrocontroller 40 empfangenen spektralen Daten und Seriennummer werden dann als spektrale Signatur und Seriennummer des Senders

6 zwecks zukünftigem Vergleich für alle folgenden Kommunikationen zwischen dem Schlüssel 4 und dem Empfänger 10 gespeichert.

Der Schlüssel 4 und die Basisstation 8 führen dann dementsprechend die folgenden Schritte durch, wenn eine Kommunikationsverbindung in der Folge hergestellt wird:

(i) Vor der Übermittlung irgendwelcher Authentifizierungsdaten werden die zwei Grundtöne in den Kanälen C2 und C3 simultan mit der Seriennummer in einem der Kanäle C2 oder C3 übermittelt.

(ii) Der Frequenzsynthetisator 42 wählt die vier Kanäle C1 bis C4 und der FM-Empfänger 36 erzeugt eine RSSI-Ausgabe für jeden der Kanäle und eine "Daten-erhalten-Ausgabe" (data received output) für den Mikrocontroller 40.

(iii) Der Mikrocontroller 40 empfängt und verarbeitet die spektralen Daten, die für die empfangenen Signalpegel für jeden der Kanäle repräsentativ sind, und dies wird mit der gespeicherten spektralen Signatur verglichen.

(iv) Falls eine Abweichung zwischen der spektralen Signatur und den spektralen Daten besteht, die mehr als ±1 % darstellt, veranlaßt der Mikrocontroller 40 die Basisstation 8 dazu, das Authentifizierungsverfahren abzubrechen und Zugang zu dem gesicherten Ort und/oder Benutzung des Fahrzeugs zu verhindern.

(v) Der Mikrocontroller 40 verarbeitet jegliche Signale auf der "Daten-erhalten-Ausgabe" um festzustellen, ob sie einen Anfangskennsatz darstellen und die gespeicherte Seriennummer enthalten. Falls die Daten auf der "Daten-erhalten-Ausgabe" mit der gespeicherten Seriennummer nicht übereinstimmen, oder der Mikrocontroller 40 eine Verzögerung entdeckt, welche die zulässige Zeitspanne zwischen der Durchführung von Schritt (iii) und Empfang von mit den gespeicherten Seriennummerndaten übereinstimmenden Daten überschreitet, verursacht der Mikrocontroller 40 die Basisstation 8, das

Authentifizierungsverfahren abzubrechen und den Zugang zu dem gesicherten Ort und/oder Starten des Fahrzeugs zu verwehren. Die Verzögerung entspricht jeder versuchten Verhinderung oder Unterdrückung von Übertragung der Seriennummer, wenn ein Zweitschlüssel 4 anfänglich erregt wird. Genauer gesagt entspricht die Verzögerung dem Empfang von mehr als einem Anfangskennsatz, bevor zu verarbeitende Daten gemäß dem Kommunikationsprotokoll empfangen werden.

(vi) Die Höhe der Abweichung der empfangenen spektralen Daten von der spektralen Signatur wird für nachfolgende Analyse aufgezeichnet, um einen charakteristischen Auffangpunkt dritter Ordnung zu ermitteln, damit die angreifende Station identifiziert werden kann. Jegliche empfangene ungenehmigte Seriennummer eines unbefugten Schlüssels wird auch gespeichert, um den unbefugten Schlüssel zu identifizieren. Die Anzahl der Angriffe kann auch gespeichert werden.

(vii) Wenn die Basisstation 8 in der Folge einen befugten Benutzer entdeckt und befugten Zugang und/oder Start des Fahrzeugs erlaubt, verursacht der Mikrocontroller 40 die Erzeugung eines Warnsignals zur Anzeige, daß ein Angriff unternommen wurde. Das Warnsignal kann in Form einer Wortanzeige, einer Warnlampe oder eines Tonsignals sein, welches an dem gesicherten Ort, d.h. dem Fahrzeug, erzeugt wird.

Um den Schlüssel 4 zu erregen, schließt die Basisstation 8 einen FM-Sender 37 ein, welcher die Antenne 12 benutzt, um die Kennungsabfragedaten 50 an den Empfänger 9 des Schlüssels 4 weiterzuleiten. Die Kennungsabfragedaten 50, wie in Figur 3 gezeigt, werden zu einem Zeitpunkt T_{Start} gesandt, zu welchem Zeitpunkt der Empfänger 36 der Basisstation 8 mit der Messung der zulässigen Zeitperiode beginnen kann, innerhalb welcher Zeitperiode die Authentifizierungsdaten von dem Schlüssel 4 her erhalten werden müssen. Der

Schlüssel 4 überträgt die Authentifizierungsdaten und die Seriennummer auf einem der verfügbaren Kanäle C2 und C3 in einer Antwortnachricht 52, wie in Figur 3 gezeigt. Die Antwortnachricht 52 wird während oder nach Übertragung der Kennungsabfrage 50 gesandt. Mindestens ein Teil der Antwortnachricht 52 muß von der Basisstation 8 innerhalb eines Abnahmezeitausschnitts 54 zwischen den Zeiten T_{MIN} und T_{MAX} empfangen werden. Die benutzten Frequenzkanäle C2 und C3 werden mittels in der Kennungsabfrage 50 enthaltene Daten ausgewählt. Die Zeit T_{START} entspricht dem Start 56 der Kennungsabfragedaten 50, und die Antwort 52 muß gültig sein und mindestens zum Teil nicht früher als T_{MIN} und nicht später als T_{MAX} empfangen werden. Falls eine Antwort 58 außerhalb des Zeitausschnitts 54 empfangen wird, ist sie automatisch eine ungültige Antwort 58. Der Beginn des Zeitausschnitts 54, T_{MIN} kann bei T_{START} oder während oder nach der Kennungsabfrage 50 oder am Ende der Kennungsabfrage 50, wie in Figur 3 gezeigt, liegen. T_{MAX} liegt ungefähr 1 Millisekunde von T_{MIN}, so daß der Abnahmezeitausschnitt 54 in etwa 1 Millisekunde entspricht. Dies ist besonders vorteilhaft, da jeder unbefugte Benutzer mit einer Angriffsstation 16 mindestens 2 bis 5 Millisekunden braucht, um die Übertragungsfrequenz für die Antwort 52 zu bestimmen, um die Antwort 52 abfangen zu können. Der Zeitausschnitt 54 ist dementsprechend so gelegt, daß er nur gültige Antworten 52 entdeckt und nicht verzögerte ungültige Antworten 58, die von einer Angriffsstation 16 erzeugt werden.

Dem Fachkundigen werden hierzu eine Vielzahl von Abwandlungen gegenwärtig werden, ohne daß der Umfang der vorliegenden Erfindung, wie sie hiermit unter Bezug auf die beiliegenden Zeichnungen beschrieben wird, überschritten wird.

ANSPRÜCHE

1. Ein Sicherheitssystem, welches einen elektronischen Schlüssel mit einem Sender und einen gesicherten Gegenstand mit einem Empfänger einschließt, worin der Sender und der Empfänger so ausgelegt sind, daß sie miteinander kommunizieren, um Authentifizierungsdaten zu übertragen, **dadurch gekennzeichnet**, daß der Sender Identifizierungsdaten übermittelt, die für den Schlüssel eindeutig sind, wobei die Identifizierungsdaten in Hardware des Senders eingebettet sind und das Sicherheitssystem eine Befugnis für den gesicherten Gegenstand bei Übertragung der Authentifizierungsdaten gewährt, wenn die übertragenen Identifizierungsdaten den Identifizierungsdaten des Empfängers entsprechen.

2. Ein Sicherheitssystem gemäß Anspruch 1, worin die Befugnis gewährt wird, wenn die Identifizierungsdaten innerhalb einer zulässigen Zeitperiode erhalten werden und den Identifizierungsdaten des Empfängers entsprechen.

3. Ein Sicherheitssystem gemäß Anspruch 2, worin die Identifizierungsdaten in einem Anfangskennsatz einer Kommunikationsnachricht zwischen dem Empfänger und dem Sender übertragen werden und der Anfangskennsatz innerhalb der zulässigen Zeitperiode empfangen werden muß, damit die Befugnis erteilt wird.

4. Ein Sicherheitssystem gemäß Anspruch 3, worin der Anfangskennsatz von dem Schlüssel in einer Antwortnachricht auf eine von dem gesicherten Gegenstand empfangene Kennungsabfrage übertragen wird, und worin mindestens ein Teil der Antwortnachricht innerhalb einer zulässigen Zeitperiode empfangen werden muß, damit die Befugnis erteilt wird.

5. Ein Sicherheitssystem gemäß Anspruch 4, worin die zulässige Zeitperiode einen Abnahmezeitausschnitt darstellt, der zu dem Übertragungsbeginn der Kennungsabfrage oder zu einer vorbestimmten Zeitperiode ab dem Übertragungsbeginn der Kennungsabfrage beginnt.

6. Ein Ein Sicherheitssystem gemäß Anspruch 5, worin die vorbestimmte Zeitperiode kleiner ist als die Länge der Kennungsabfrage oder der Länge der Kennungsabfrage gleich ist.

7. Ein Sicherheitssystem gemäß Anspruch 6, worin der Abnahmezeitausschnitt in etwa 1 Millisekunde entspricht.

8. Ein Sicherheitssystem gemäß einem der vorangegangenen Ansprüche, worin der Sender eine integrierte Schaltung einschließt, in welcher die Identifizierungsdaten eingebettet sind.

9. Ein Sicherheitssystem gemäß einem der vorangegangenen Ansprüche, worin der Sender auf die Identifizierungsdaten Zugriff nimmt und diese überträgt, wenn er eine Übertragung an den Empfänger beginnt.

10. Ein Sicherheitssystem gemäß Anspruch 9, worin die eindeutigen Identifizierungsdaten eine Seriennummer für den Schlüssel darstellen und automatisch ungeachtet anderer zur Übertragung an den Sender gelieferten Daten übertragen werden.

11. Ein Sicherheitssystem gemäß Anspruch 9 in Abhängigkeit von mindestens Anspruch 2, worin der Sender ein Tonsignal übermittelt, welches der Sender in spektrale Daten umwandelt, und das Sicherheitssystem Befugnis bei Übertragung der Authentifizierungsdaten gewährt, wenn die spektralen Daten mit der spektralen Signatur des Senders übereinstimmen, und die übertragenen Identifizierungsdaten mit den Identifizierungsdaten des Empfängers übereinstimmen und in der zulässigen Zeitperiode empfangen werden.

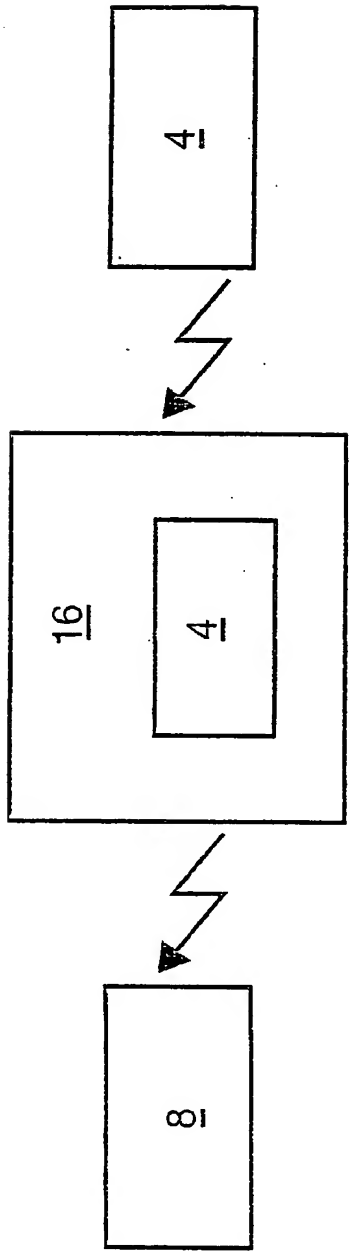


FIGURE 1

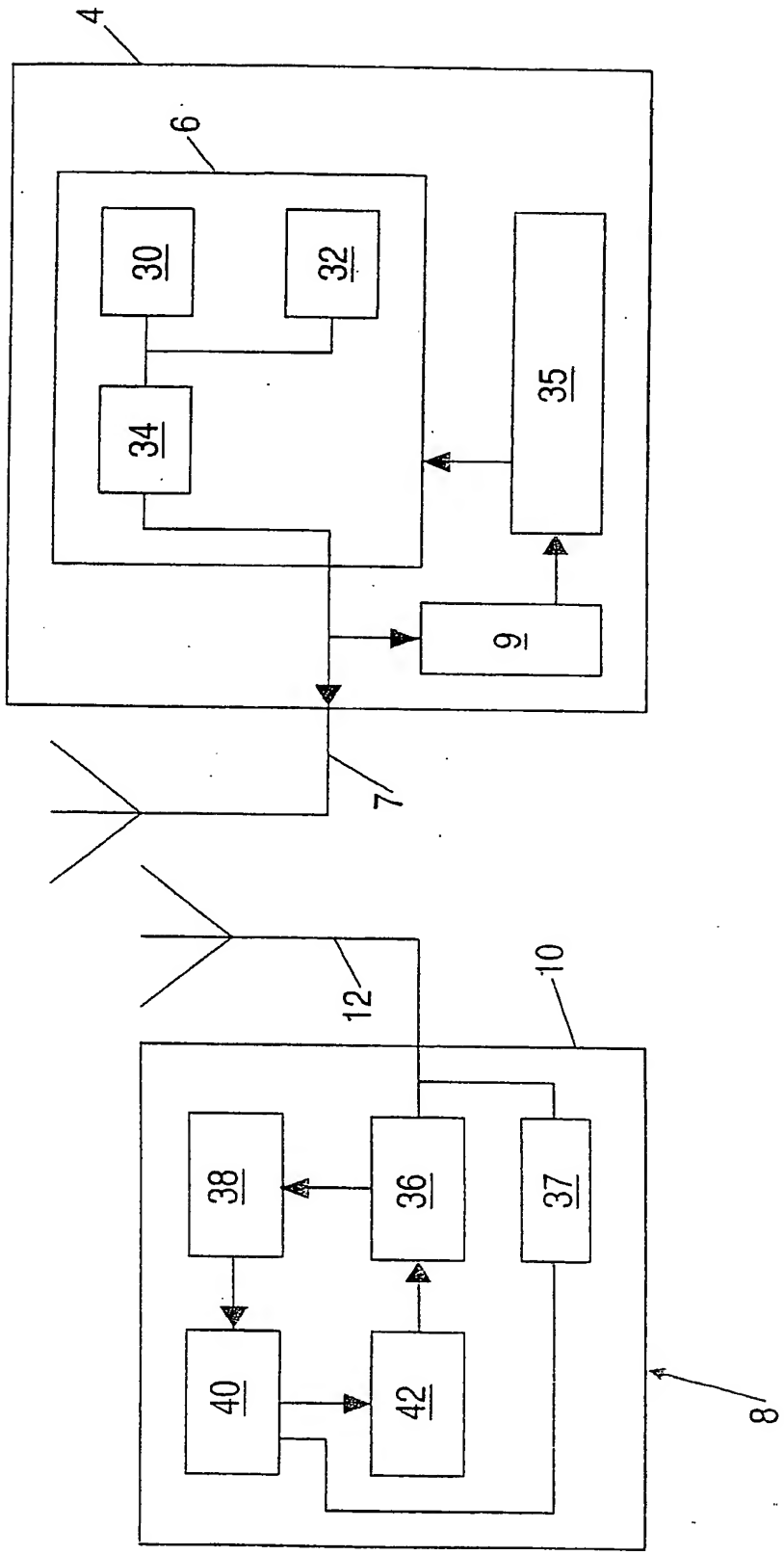


FIGURE 2

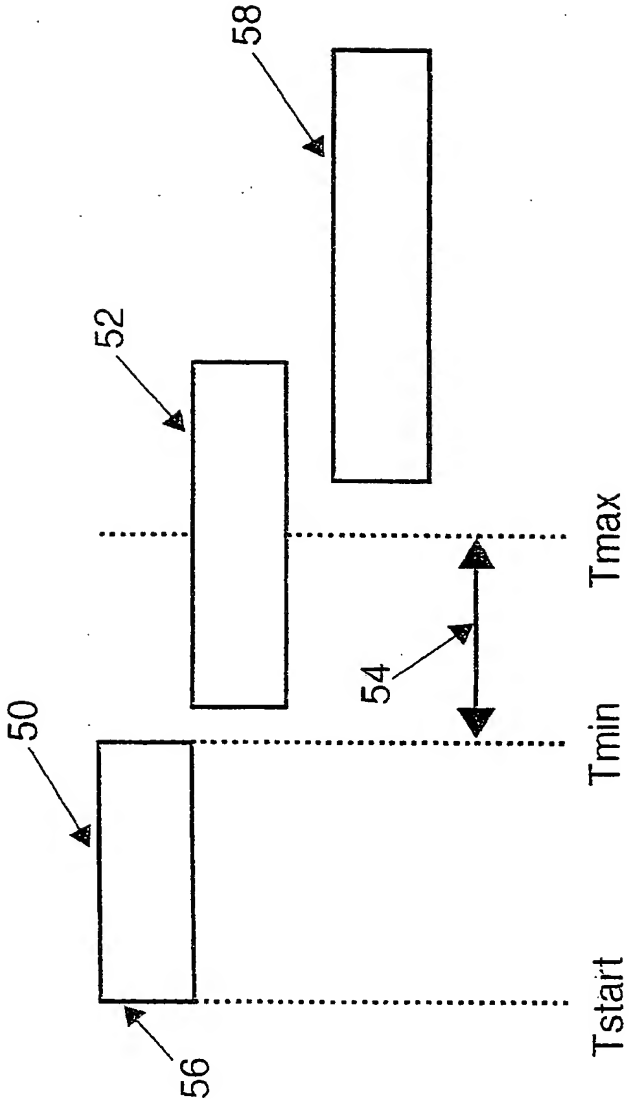


FIGURE 3

INTERNATIONAL SEARCH REPORT

Internati , Application No
PCT/DE 99/02619

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 770 749 A (VALEO SECURITE HABITACLE) 2 May 1997 (1997-05-02) abstract; figure 1 column 2, line 48 -column 3, line 8 column 4, line 36 - line 45	1,8,9
Y		2
A		10
X	EP 0 831 197 A (TRW INC) 25 March 1998 (1998-03-25) abstract; figure 1 column 13, line 46 -column 14, line 6	1,8-10
Y	DE 40 20 445 A (BAYERISCHE MOTOREN WERKE AG) 2 January 1992 (1992-01-02) the whole document	2

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 February 2000	22/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Form PCT/ISA/210 (second sheet) (July 1992)

BEST AVAILABLE COPY

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatk Application No
PCT/DE 99/02619

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0770749 A	02-05-1997	FR 2740500 A	30-04-1997
		FR 2740501 A	30-04-1997
		DE 29623461 U	23-07-1997
		JP 9177401 A	08-07-1997
		US 5929769 A	27-07-1999
EP 0831197 A	25-03-1998	DE 3856232 D	17-09-1998
		DE 3856232 T	22-04-1999
		EP 0292217 A	23-11-1988
		JP 9324567 A	16-12-1997
		JP 7091913 B	09-10-1995
		JP 63308171 A	15-12-1988
		US 5406274 A	11-04-1995
		US 4881148 A	14-11-1989
		US 5109221 A	28-04-1992
		US 5619191 A	08-04-1997
		US 5774064 A	30-06-1998
		US 5252966 A	12-10-1993
DE 4020445 A	02-01-1992	DE 4003280 A	08-08-1991
		DE 59009066 D	14-06-1995
		EP 0440974 A	14-08-1991
		ES 2071738 T	01-07-1995

BEST AVAILABLE COP'

INTERNATIONALER RECHERCHENBERICHT

Internat. ...es Aktenzeichen
PCT/DE 99/02619

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B49/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 770 749 A (VALEO SECURITE HABITACLE) 2. Mai 1997 (1997-05-02) Zusammenfassung; Abbildung 1 Spalte 2, Zeile 48 -Spalte 3, Zeile 8 Spalte 4, Zeile 36 - Zeile 45	1,8,9
Y		2
A		10
X	EP 0 831 197 A (TRW INC) 25. März 1998 (1998-03-25) Zusammenfassung; Abbildung 1 Spalte 13, Zeile 46 -Spalte 14, Zeile 6	1,8-10
Y	DE 40 20 445 A (BAYERISCHE MOTOREN WERKE AG) 2. Januar 1992 (1992-01-02) das ganze Dokument	2

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahellegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche	Absendedatum des Internationalen Recherchenberichts
14. Februar 2000	22/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Buron, E

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

BEST AVAILABLE COP

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internatio. › Aktenzeichen
PCT/DE 99/02619

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0770749	A	02-05-1997	FR	2740500 A	30-04-1997
			FR	2740501 A	30-04-1997
			DE	29623461 U	23-07-1997
			JP	9177401 A	08-07-1997
			US	5929769 A	27-07-1999
EP 0831197	A	25-03-1998	DE	3856232 D	17-09-1998
			DE	3856232 T	22-04-1999
			EP	0292217 A	23-11-1988
			JP	9324567 A	16-12-1997
			JP	7091913 B	09-10-1995
			JP	63308171 A	15-12-1988
			US	5406274 A	11-04-1995
			US	4881148 A	14-11-1989
			US	5109221 A	28-04-1992
			US	5619191 A	08-04-1997
			US	5774064 A	30-06-1998
			US	5252966 A	12-10-1993
DE 4020445	A	02-01-1992	DE	4003280 A	08-08-1991
			DE	59009066 D	14-06-1995
			EP	0440974 A	14-08-1991
			ES	2071738 T	01-07-1995

BEST AVAILABLE COPY